(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067531 A1

(51) International Patent Classification⁷: H04L 29/06, 29/12

(21) International Application Number: PCT/CA02/00214

(22) International Filing Date: 19 February 2002 (19.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/269,357 20 February 2001 (20.02.2001) US

(71) Applicant *(for all designated States except US)*: **EYEBALL NETWORKS INC.** [CA/CA]; 500 - 100 Park Royal, West Vancouver, British Columbia V7T 1A2 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **PICHE, Christopher** [CA/CA]; 500 - 100 Park Royal, West Vancouver, British Columbia V7T 1A2 (CA). **KHAN, Md. Shahadatullah** [BD/CA]; 1102-145 St. Georges Avenue, North Vancouver, British Columbia V7L 3G8 (CA). **MARWOOD, David, Everett** [CA/CA]; 863 Westview Crescent, North Vancouver, British Columbia V7N 3X9 (CA). **CHUNG, Michael** [CA/CA]; 1495 Johnson Road, RR6, Gibsons, British Columbia V0N 1V6 (CA).

(74) Agent: **GREEN, Bruce, M.**; c/o Oyen Wiggs Green & Mutala, 480 - 601 West Cordova Street, Vancouver, British Columbia V6B 1G1 (CA).

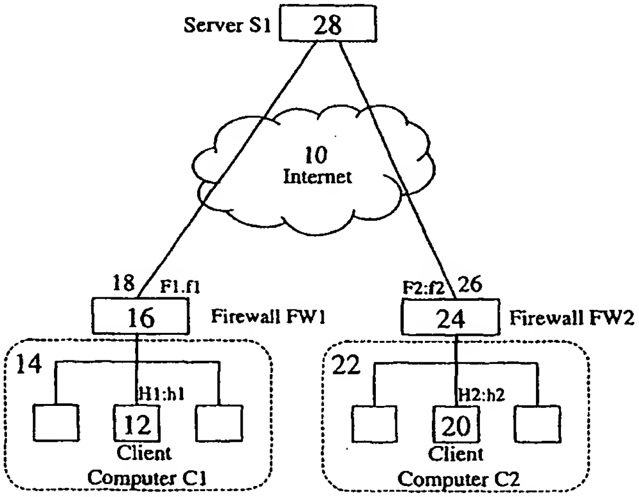
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS TO PERMIT DATA TRANSMISSION TO TRAVERSE FIREWALLS



(57) **Abstract:** Currently data transmission over the Internet between two client computers where both client computers are protected by firewalls is problematic, since firewalls block incoming packets. A method is provided for permitting packet based data transmission between a first client computer C1 protected by a first NAPT or NAT firewall and a second client computer C2 protected by a second NAPT or NAT firewall to traverse the first and the second firewalls. The method can also be applied to other devices, such as routers, using NAT or NAPT.

METHOD AND APPARATUS TO PERMIT DATA TRANSMISSION TO TRAVERSE FIREWALLS

Related application

This application claims priority from previously filed United States provisional patent application serial number 60/269,357, filed February 20, 2001, entitled METHOD AND APPARATUS TO PERMIT REAL-TIME MEDIA DELIVERY TO TRAVERSE FIREWALLS ON A COMPUTER NETWORK.

Technical Field

The invention relates to the field of data transmission over a computer network, and more particularly to methods for permitting data transmissions using packet based transmission protocols to traverse firewalls.

Background Art

Computers connected to wide area networks like the Internet are commonly protected by firewalls. Firewalls are most commonly used to protect computers operating on local area networks, but they can also be used to protect individual computers, including servers, which access a wide area network. In this application, the term “client computer” will encompass any computer with access to a wide area network, and also a program operating on such a computer. Such a computer may, but need not, operate on a local area network, and may perform the functions of a server on the wide area network.

Firewalls typically perform a number of functions. They protect internal computers from outside computers on the wide area network, while allowing internal computers to access the wide area network. Firewalls can also make local network administration more efficient, by permitting a large number of client computers to share a limited pool of Internet Protocol (IP) addresses on the wide area network, and by accommodating changes within the local network without having to re-configure access to the other computers on the wide area network.

A firewall is typically a program or collection of related programs on a network gateway server which check each network packet to determine whether to forward it to its destination. To create a barrier between an internal computer and the outside wide area network, firewalls commonly use NAT (network address translation) or NAPT (network address and port translation). NAT is the translation of an internal IP address used by a client computer (and known within the internal network, if the client computer is operating on one), to a different IP address known within the outside wide area network. The firewall maps internal IP addresses to one or more global external IP addresses, and reverse maps the external IP addresses on incoming packets back into internal IP addresses. NAPT is the translation of both internal IP addresses and internal ports to different external IP addresses and external ports known within the outside network. Firewalls using NAPT commonly screen incoming packets to make sure that they come from a previously identified IP address and port. That is, a request from a particular IP address and port traverses the firewall only if a request previously went out from the firewall to that IP address and port.

Data transmission over the Internet has become an everyday occurrence. Many Internet data transmissions are used to transport audio and / or video data from a live or on-demand streaming server to streaming clients, to provide real-time interactive communication (such as "chat") between client computers, to transport the contents of web-pages from web-servers to web-clients, and for many other types of communication among networked programs. Different protocols are used to transmit different types of data. For example, text chat is generally transmitted using Transmission Control Protocol (TCP), while audio / video conferencing and live audio / video streaming are generally transmitted using UDP (User Datagram Protocol). Communications through a server connected directly to the Internet (that is, not behind a firewall) are not generally obstructed by client-side firewalls; the act of logging on to a server generally opens a return path from the server through the firewall. However, firewalls commonly block direct client-to-client, or "peer-to-peer" communication. One attempted solution is to open certain ports in the firewall, but this solution (i) requires modification of the firewall settings, which most network administrators are reluctant to do, and (ii) does not work with firewalls that perform any sort of port translation. The present invention provides a method for permitting packet based data transmission to traverse firewalls using either NAPT or NAT without altering firewall settings. The invention is disclosed in the context of a firewall using NAPT, as the more general case. However, the method provided in the invention is equally applicable to a firewall using NAT, and also to other types of devices, such as routers, using either NAPT or NAT

Disclosure of Invention

The invention therefore provides a method of transmitting a data packet from a first computer to a second computer over a wide area computer network, a data packet transmitted from the first computer having a first source address designating the first computer and a data packet transmitted from the second computer having a second source address designating the second computer, wherein the first computer is protected by a first firewall which translates the first source address to a first external address when transmitting a data packet from the first computer to the wide area network, and the second computer is protected by a second firewall which translates the second source address to a second external address when transmitting a data packet from the second computer to the wide area network, the first and second firewalls communicating over the wide area computer network, the method using a designated recipient computer in communication with the first and second computers via the wide area computer network, said method comprising: a) the first and second computers sending first and second data packets to the designated recipient computer; b) the designated recipient computer communicating the first external address from the first data packet to the second computer and communicating the second external address from the second data packet to said first computer; c) the second computer sending a data packet to the first external address; and d) the first computer sending a data packet to said second external address.

The method further provides for two-way transmission of data by additionally having the second computer then send a data packet to the first external address. The method can be applied to a plurality of computers protected by firewalls communicating over a wide area network. The firewalls may be NAT or NAPT. In particular the method works if the IP address and port are translated at the firewall, or only the IP address. The designated recipient computer can be any type of computer, including without limitation a designated server, a peer computer involved in the data transmission, or a peer computer not involved in the data transmission.

The present invention further provides a computer program product for carrying out the foregoing method, and a system for transmitting a data packet between two firewall-protected computers over a wide area network,

Brief Description of Drawings

Figure 1 is a schematic diagram illustrating a preferred embodiment of the invention; and

Figure 2 is a flowchart illustrating a preferred embodiment of the invention.

Best Mode(s) for Carrying Out the Invention

Fig. 1 schematically illustrates a client computer C1 (12) on local area network (14), protected by NAPT firewall FW1 (16), wishing to send a UDP data stream, such as a live video data stream, over Internet 10, to client computer C2 (20) on local area network (22), protected by NAPT firewall FW2 (24). Within this schematic, C1 has internal IP address H1, and will use internal port h1 to transmit the UDP data stream. Firewall FW1 translates these into external IP address F1 and external port f1 (18). C2 has internal IP address H2, and will use internal port h2 to receive the UDP data stream. Firewall FW2 will receive UDP packets destined for C2 at external IP address F2 and external port f2 (26). Both C1 and C2 log onto a server S1 (28), whose purpose is to establish a path to transmit the UDP data stream from C1 to C2. However, the UDP data stream is not transmitted through the server. It is sent client-to-client to take advantage of efficiencies and scalability that can be realized from peer-to-peer communication over the Internet.

Peer-to-peer communications are prevented by almost all firewalls. NAPT firewalls FW1 and FW2 will only permit an incoming UDP packet to pass if (i) its source and destination addresses match the destination and source addresses, respectively, of a recent outgoing UDP packet, and (ii) its source and destination ports match the destination and source ports, respectively, of a recent outgoing UDP packet. If either C1 or C2 attempts to send a packet to the other, the receiver's firewall will block the incoming packet if it does not meet these criteria.

The present invention permits C1 to send a UDP data stream to C2 by the following steps:

(1) C1 sends a UDP packet U1 to server S1. C1 initiates the transmission from its internal IP address and UDP port (H1:h1). Firewall FW1 translates the IP address and port to F1:f1 at the external interface of FW1.

(2) When S1 receives packet U1 from F1:f1, S1 can identify F1 and f1 as the external IP address and external port from which FW1 will send the UDP data stream originating with C1.

(3) C2 sends a UDP packet U2 to server S1. C2 initiates the transmission from its internal IP address and UDP port (H2:h2). Firewall FW2 translates the IP address and port to F2:f2 at the external interface of FW2.

(4) When S1 receives packet U2 from F2:f2, S1 can identify F2 and f2 as the external IP address and external port at which FW2 will receive the UDP data stream to be transmitted from C1 to C2.

(5) S1 tells C2 that F1:f1 are the external IP address and port from which C1 will send the UDP data stream.

(6) S1 tells C1 that F2:f2 are the external IP address and port to which the UDP data stream destined for C2 should be sent.

(7) C2 sends a UDP packet U3 to F1:f1, using its internal port h2. Firewall FW2 will send the packet from F2:f2. This packet will be blocked by firewall FW1. However, as described in step (8), it will prompt firewall FW2 to pass subsequent packets sent by C1 destined for C2.

(8) When C1 subsequently sends a data stream consisting of UDP packets destined for C2 from its internal port h1, firewall FW1 will send them from F1:f1 to F2:f2. Because of the packet sent in step (7), firewall FW2 recognizes F1:f1 as an address and port to which it has recently sent a packet from F2:f2. Accordingly, it permits packets sent from F1:f1 to F2:f2 to pass through the firewall, and forwards them to H2:h2, the internal IP address and port for C2.

In this way, the invention creates a means by which UDP data streams originating with C1 pass through to C2. This can be used for streaming applications, in which C1 sends a live or on-demand data stream to C2. Steps similar to (1) to (8), carried out vice versa, will permit UDP data streams originating with C2 to pass through firewall F1, to C1. Thus, C1 and C2 can utilize applications which depend on two-way transmission of UDP data streams, such as video conferencing. Similar steps carried out by a number of client computers, C1,...,CN, will permit one-to-many, many-to-one, or many-to-many transmission of UDP data streams through NAPT firewalls.

For the method to work with a firewall using NAPT, the packets sent in steps (1) and (3) will generally have to be of the same type (i.e. TCP, UDP, etc.) as the type used to transmit the data in step (8). The reason is that many computer applications or firewalls use different ports to transmit and receive different types of data. However, if that is not the case, the packets sent in steps (1) and (3) need not be of the same type as the type used in step (8). In addition, firewall FW1 must use the same external IP address and port to send the initial packet in step (1) as it uses subsequently to commence sending the data to C2 in step (8) (although the method can be adapted to accommodate subsequent changes in the IP addresses and ports, as described more fully below). This generally happens in practice so long as the software at client computer C1 is written to send both transmissions from the same internal IP address and port, as most firewall programs using NAPT currently create one-to-one mappings between internal IP addresses and ports and external IP addresses and ports used to send the same type of packet. Similarly, firewall FW2 must use the same external IP address and port to send the packet in step (3) that it will use to commence receiving the data in step (8). This also will generally happen in practice, so long as the software at client computer C2 is written to send the packet in step (3) from, and to receive the data in step (8) at, the same internal IP address and port.

As will be apparent to those skilled in the art, the method can be readily adapted to support two-way data transmission between C1 and C2, to support one-to-many data transmission from C1 to client computers C2,...,CN, to support many-to-one data transmission from client computers C2,...,CN to C1, or to support many-to-many data transmission among client computers C1,...,CN. As well, the invention has been described with both C1 and C2 protected by firewalls, as that situation provides the clearest description of the invention. However, the method is readily adapted to the situation where only the receiving client computer is protected by a firewall.

The designated recipient computer can be any type of computer, including without limitation a designated server, a peer computer involved in the data transmission, or a peer computer not involved in the data transmission.

As will be apparent to those skilled in the art in light of the foregoing disclosure, many alterations and modifications are possible in the practice of this invention without departing from the spirit or scope thereof. For example, the possible alterations and modifications include, but are not limited to, the following:

1. For robustness against packet loss or delay, C1 and /or C2 could send multiple packets to S1 in steps (1) and (3), instead of a single packet. Packets could be sent until confirmation is received that S1 has received one of the packets.

2. Also for robustness against packet loss or delay, C2 could send multiple packets in step (7), instead of a single packet. Packets could be sent until confirmation is received that FW1 has received one of the packets.

3. The method can also be used when either C1 or C2 uses separate ports for sending and receiving UDP data streams. For example, if C1 uses h1 for sending UDP data streams and h3 for receiving data streams, firewall FW1 will translate these into f1 and f3 respectively. C2 would have to send a UDP packet from its receiving port to f1, and C1 would have to send a UDP packet from f3 to the sending port for C2. These packets would open paths over which C1 could send to C2 (through f1), and over which C2 could send to C1 (through f3).

4. In the case of two-way communication, and where firewalls FW1 and FW2 use the same external ports for both sending and receiving UDP data, the initial data packets in the data streams can be used as the packets required to open the paths (as in step (7)). The initial data packets may be blocked, until a data packet is sent in the other direction. However, applications using UDP transmissions are typically robust against packet loss, and the method will work so long as loss of the initial data packet or packets is not critical to the application in question.

5. If firewall FW1 (or FW2) changes the external IP address or port which it uses to transmit UDP data for any reason (such as a long data transmission or period of silence), the method can be adapted to refresh the data identifying the external IP addresses and ports, to maintain open transmission paths. For example, if FW1 changes the external IP address or port used to transmit UDP data originating from C1, new packets will be sent periodically to the intermediary server S1 as in step (1), above, to identify any new IP address or port being used by FW1. The remaining steps (2) through (8) can then be repeated using new data. All that the method requires is that the same external sending IP address and port be used by FW1 for a long enough period of time that the initial packet sent to S1 in step (1) come from the same IP address and port as the initial data packets in the UDP data stream.

6. In the best mode described above, server S1 is used as intermediary to receive UDP packets originating from C1 and C2, and to use information contained in those packets to identify the external ports being used by FW1 and FW2. However, any other means for informing each terminal of the other's external ports will also work according to the invention. For example, C1 and C2 could use different echo servers, S1 and S2, which return any UDP packet to its source. This will permit C1 and C2 to identify F1:f1 and F2:f2, respectively. C1 and C2 could use any other means, such as off-line exchange of information by

the users, or TCP transmissions either directly to the other or through a common server, to inform each other about F1:f1 and F2:f2.

7. The method can be used where client computers communicate through a server computer, although the method is not usually needed in that case, as a client computer generally opens a return path from the server when it logs on to the server.

8. The method can also be used where only the receiving client computer is behind a firewall, but there is no firewall protecting the sending client computer.

9. Although the above method has been described in the context of real-time audio and video communications using UDP packets, it will be apparent to those skilled in the art that the method has application to other forms of packet based data transmission.

10. The method can also be adapted to firewalls which do not create one-to-one mappings between internal and external IP addresses and ports, by deducing the mapping scheme from received packets, and then utilizing the deduced mapping schemes to send the required packets from the external receiving IP addresses and ports of each client computer to the external sending IP addresses and ports of each other client computer.

11. While the invention has been disclosed in connection with a NAPT firewall, it would also operate in the same manner if firewalls FW1 and FW2 are NAT firewalls. In that case, NAT FW1 would translate H1:h1 to F1:h1, and NAT FW2 would translate H2:h2 to F2:h2. The method would otherwise be identical.

WHAT IS CLAIMED IS:

1. A method of transmitting a data packet from a first computer to a second computer over a wide area computer network, a data packet transmitted from said first computer having a first source address designating said first computer and a data packet transmitted from said second computer having a second source address designating said second computer, wherein said first computer is protected by a first firewall which translates said first source address to a first external address when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which translates said second source address to a second external address when transmitting a data packet from said second computer to said wide area network, said first and second firewalls communicating over said wide area computer network, said method using a designated recipient computer in communication with said first and second computers via said wide area computer network, said method comprising:

a) said first and second computers sending first and second data packets to said designated recipient computer;

b) said designated recipient computer communicating said first external address from said first data packet to said second computer and communicating said second external address from said second data packet to said first computer;

c) said second computer sending a data packet to said first external address; and

d) said first computer sending a data packet to said second external address.

2. A method for permitting two-way transmission of data packets between a first computer and a second computer over a wide area computer network, a data packet transmitted from said first computer having a first source

address designating said first computer and a data packet transmitted from said second computer having a second source address designating said second computer, wherein said first computer is protected by a first firewall which translates said first source address to a first external address when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which translates said second source address to a second external address when transmitting a data packet from said second computer to said wide area network, said first and second firewalls communicating over said wide area computer network, said method using a designated recipient computer in communication with said first and second computers via said wide area computer network, said method comprising:

a) said first and second computers sending first and second data packets to said designated recipient computer;

b) said designated recipient computer communicating said first external address from said first data packet to said second computer and communicating said second external address from said second data packet to said first computer;

c) said second computer sending a first data packet to said first external address;

d) said first computer sending a data packet to said second external address; and

e) said second computer sending a second data packet to said first external address.

3. A method for permitting two-way transmission of data packets between any two of a plurality of computers over a wide area computer network, a data packet transmitted from each computer having a source address designating said computer, wherein each computer is protected by a firewall which translates said source address of said computer to an external address when transmitting a data packet from said computer to said wide area network, said firewalls

communicating over said wide area computer network, said method using a designated recipient computer in communication with said plurality of computers via said wide area computer network, said method comprising:

a) said plurality of computers sending respective data packets to said designated recipient computer;

b) said designated recipient computer communicating the respective external addresses from said data packets to said plurality of computers;

c) a first of said plurality of computers having a first external address sending a first data packet to a second external address associated with a second of said plurality of computers;

d) said second computer sending a data packet to said first external address; and

e) said first computer sending a second data packet to said second external address.

4. The method of Claims 1 or 2 wherein a data packet transmitted from said first computer further has a first port designating said first computer and a data packet transmitted from said second computer has a second port designating said second computer, and said first firewall further translates said first port to a first external port when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which further translates said second port to a second external port when transmitting a data packet from said second computer to said wide area network.

5. The method of Claims 1 to 4 wherein said firewalls are NAPT firewalls.

6. The method of Claims 1 to 3 wherein said firewalls are NAT firewalls.

7. The method of Claims 1 to 3 wherein said data packets consist of UDP data streams.

8. The method of Claims 1 to 3 wherein said data packets consist of live audio / video data streams.

9. The method of Claims 1 to 3 wherein said data packets consist of stored audio / video data.

10. The method of Claims 1 to 3 wherein said data packets consist of the contents of a stored computer file.

11. The method of Claims 1 to 3 wherein said data packets consist of data streams carrying audio / video conferencing communication.

12. The method of Claims 1 to 3 wherein multiple data packets are sent by said first and second computers in step (a).

13. The method of Claims 1 to 3 wherein multiple data packets are sent in step c).

14. The method of Claims 1 to 3 wherein multiple data packets are sent step d).

15. The method of Claims 2 or 3 wherein multiple data packets are sent in step e).

16. The method of Claims 1 or 2 wherein said first and second computers use different internal ports for sending and receiving said data packets, which internal ports get mapped to different external ports for sending and receiving said data packets, and the packets in step (c) of Claim 1, and in steps (c)

and (d) of Claim 2, are sent from the receiving port of each firewall to the sending port of the other firewall.

17. The method of Claims 1 to 3 wherein the steps therein are repeated periodically to accommodate changes in the external ports being used by some or all of the firewalls.P

18. The method of Claims 1 to 4 wherein said designated recipient computer is a common server.

19. The method of Claims 1 to 4 wherein said designated recipient computer is a peer computer involved in the data transmission.

20. The method of Claims 1 to 4 wherein said designated recipient computer is a peer computer not involved in the data transmission.

21. The method of Claims 1 to 3 wherein said designated recipient computer is an echo server, and said echo server communicates said addresses to said first and second computer by returning each packet to said first or second computer which was its source, and said first or second computer communicating said address to the other computer.

22. The method of Claims 1 to 3 wherein said first and second computers transmit data through a server computer.

23. A computer program product for transmitting a data packet from a first computer to a second computer over a wide area computer network, a data packet transmitted from said first computer having a first source address designating said first computer and a data packet transmitted from said second computer having a second source address designating said second computer, wherein said first computer is protected by a first firewall which translates said

first source address to a first external address when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which translates said second source address to a second external address when transmitting a data packet from said second computer to said wide area network, said first and second firewalls communicating over said wide area computer network, said method using a designated recipient computer in communication with said first and second computers via said wide area computer network, said computer program product comprising

a) a computer usable medium having computer read-able program code means embodied in the medium for causing said first and second computers to send first and second data packets to said designated recipient computer;

b) the computer usable medium having computer readable program code means embodied in the medium for causing said designated recipient computer to communicate said first external address from said first data packet to said second computer and communicating said second external address from said second data packet to said first computer;

c) the computer usable medium having computer readable program code means embodied in the medium for causing said second computer to send a data packet to said first external address; and

d) the computer usable medium having computer readable program code means embodied in the medium for causing said first computer to send a data packet to said second external address.

24. A computer program product for permitting two-way transmission of data packets between a first computer and a second computer over a wide area computer network, a data packet transmitted from said first computer having a first source address designating said first computer and a data packet transmitted from said second computer having a second source address designating said second computer, wherein said first computer is protected by a first firewall which

translates said first source address to a first external address when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which translates said second source address to a second external address when transmitting a data packet from said second computer to said wide area network, said first and second firewalls communicating over said wide area computer network, said method using a designated recipient computer in communication with said first and second computers via said wide area computer network, said method comprising:

a) a computer usable medium having computer read-able program code means embodied in the medium for causing said first and second computers to send first and second data packets to said designated recipient computer;

b) the computer usable medium having computer readable program code means embodied in the medium for causing said designated recipient computer to communicate said first external address from said first data packet to said second computer and communicating said second external address from said second data packet to said first computer;

c) the computer usable medium having computer readable program code means embodied in the medium for causing said second computer to send a data packet to said first external address;

d) the computer usable medium having computer readable program code means embodied in the medium for causing said first computer to send a data packet to said second external address; and

e) the computer usable medium having computer readable program code means embodied in the medium for causing said first computer to send a data packet to said second external address.

25. The computer program product of Claims 23 or 24 wherein said real-time media delivery involves live audio / video data.

26. The computer program product of Claims 23 or 24 wherein the said real-time media delivery involves stored on-demand streamed audio / video data.

27. The computer program product of Claims 23 or 24 wherein the said real-time media delivery involves the contents of a stored computer file.

28. The computer program product of Claims 23 or 24 wherein the said real-time media delivery involves audio / video conferencing communication.

29. The computer program product of Claims 23 or 24 wherein the program causes the computer on which the computer program is operating to send a UDP data packet to an intermediary for the purpose of identifying the external sending port which will be assigned to it, and receives data from the intermediary to identify the external receiving port assigned to the other participant.

30. A system for transmitting a data packet between two firewall-protected computers over a wide area network, said system comprising:

a) first and second computers adapted to communicate over a wide area computer network, wherein a data packet transmitted from said first computer has a first source address designating said first computer and a data packet transmitted from said second computer has a second source address designating said second computer, wherein said first computer is protected by a first firewall which translates said first source address to a first external address when transmitting a data packet from said first computer to said wide area network, and said second computer is protected by a second firewall which translates said second source address to a second external address when transmitting a data packet from said second computer to said wide area network, said first and second firewalls communicating over said wide area computer network,

b) a designated recipient computer in communication with said first and second computers via said wide area computer network;

wherein said first and second computers comprise means for sending first and second data packets to said designated recipient computer; said designated recipient computer comprises means for communicating said first external address from said first data packet to said second computer and communicating said second external address from said second data packet to said first computer; said second computer comprises means sending a data packet to said first external address; and said first computer comprising means for sending a data packet to said second external address.

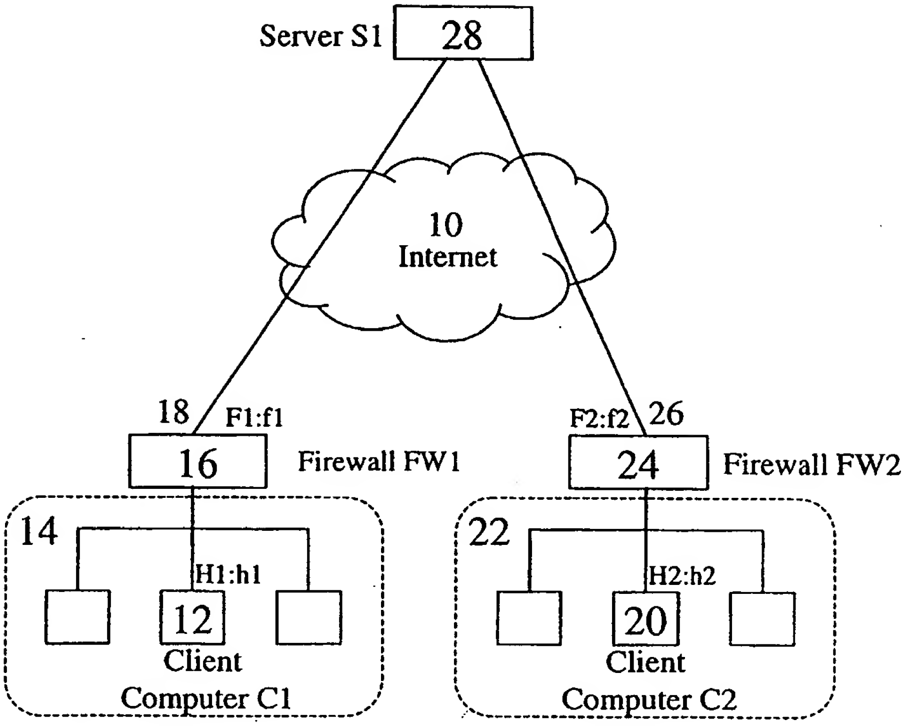

Server S1
28
10
Internet
18
F1:f1
16
Firewall FW1
F2:f2
26
24
Firewall FW2
14
H1:h1
12
Client
Computer C1
22
H2:h2
20
Client
Computer C2

FIG. 1

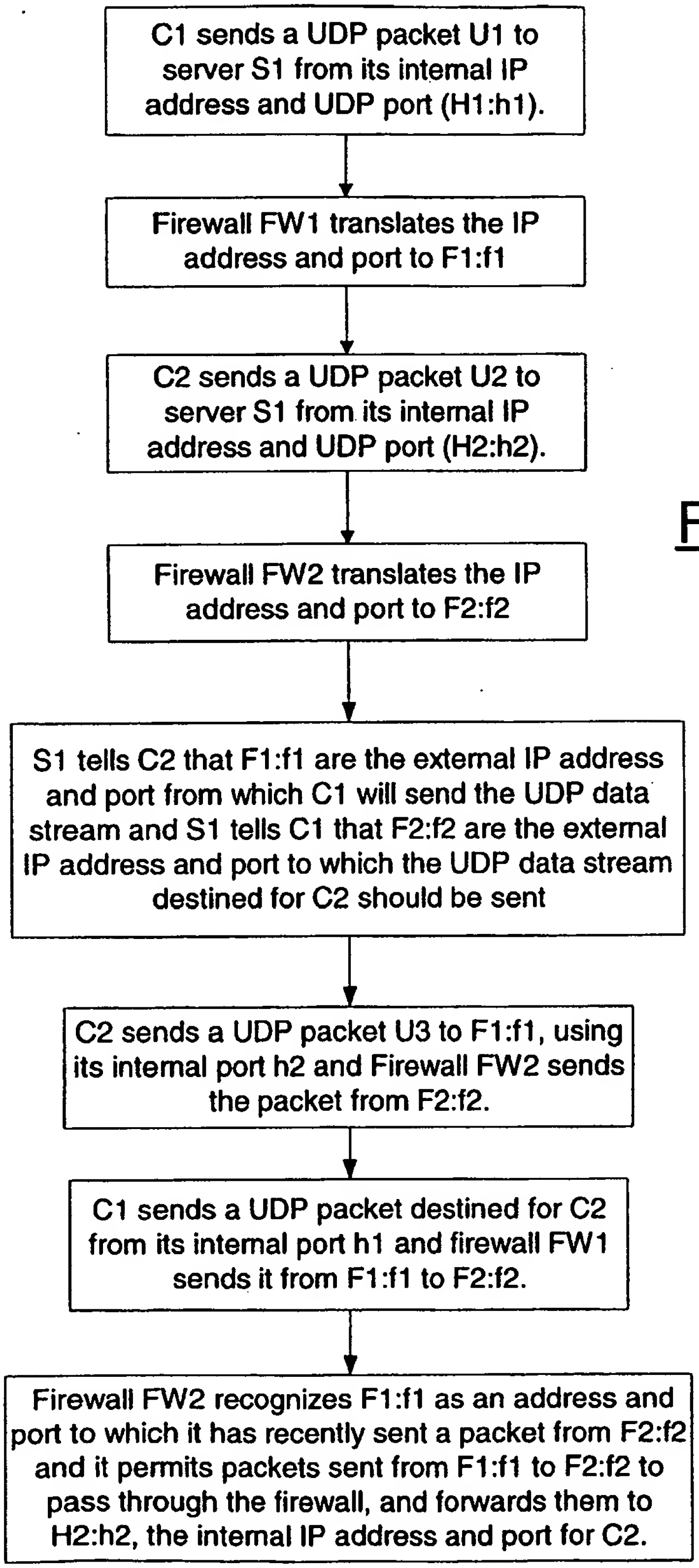

C1 sends a UDP packet U1 to server S1 from its internal IP address and UDP port (H1:h1).
Firewall FW1 translates the IP address and port to F1:f1
C2 sends a UDP packet U2 to server S1 from its internal IP address and UDP port (H2:h2).
Firewall FW2 translates the IP address and port to F2:f2
S1 tells C2 that F1:f1 are the external IP address and port from which C1 will send the UDP data stream and S1 tells C1 that F2:f2 are the external IP address and port to which the UDP data stream destined for C2 should be sent
C2 sends a UDP packet U3 to F1:f1, using its internal port h2 and Firewall FW2 sends the packet from F2:f2.
C1 sends a UDP packet destined for C2 from its internal port h1 and firewall FW1 sends it from F1:f1 to F2:f2.
Firewall FW2 recognizes F1:f1 as an address and port to which it has recently sent a packet from F2:f2 and it permits packets sent from F1:f1 to F2:f2 to pass through the firewall, and forwards them to H2:h2, the internal IP address and port for C2.

FIG. 2

INTERNATIONAL SEARCH REPORT

I tional Application No
PCT/CA 02/00214

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ESCHENBURG A: "WO LAUFEN SIE DENN? ICQ HAELT VERBINDUNG ZU BEKANNTEN" CT MAGAZIN FUER COMPUTER TECHNIK, VERLAG HEINZ HEISE GMBH., HANNOVER, DE, no. 22, 26 October 1998 (1998-10-26), pages 92-95, XP000779803 ISSN: 0724-8679 the whole document ---	1-30
Y	ROSENBERG J ET AL: "Getting SIP through Firewalls and NATs" INTERNET DRAFT, 22 February 2000 (2000-02-22), XP002167710 paragraph '02.1! paragraph '02.2! paragraph '04.1! - paragraph '04.2! paragraph '05.1! - paragraph '06.2! --- -/--	1-30

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 23 April 2002	Date of mailing of the international search report 29/04/2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Figiel, B

INTERNATIONAL SEARCH REPORT

I tional Application No
PCT/CA 02/00214

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	TSUCHIYA P F ET AL: "Extending the IP Internet through address reuse" COMPUTER COMMUNICATIONS REVIEW, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, US, vol. 1, no. 23, 1993, pages 16-33, XP002075152 ISSN: 0146-4833 paragraph ‘0002!; figure 2 page 23, line 10 - line 19 ---	1-3,23, 24,30
A	US 5 793 763 A (MAYES JOHN C ET AL) 11 August 1998 (1998-08-11) abstract; figure 2 column 4, line 55 - line 65 column 13, line 1 - line 4 -----	1,22

INTERNATIONAL SEARCH REPORT

Information on patent family members

In   ional Application No
PCT/CA 02/00214

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5793763 A	11-08-1998	US 6298063 B1	02-10-2001
		US 6317775 B1	13-11-2001
		US 6061349 A	09-05-2000
		US 6104717 A	15-08-2000